International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 11, Issue 09 (September 2015), PP.20-27

A Novel Method for Prevention of Bandwidth Distributed Denial of Service Attacks

S. Anil Kumar[1], G. Dayanandam[2], Dr. T. V. Rao[3]
[1]*Department of CSE, QISCET, Ongole, Andhra Pradesh, INDIA*
[2]*Department of CSE, Research Scholar, ANUCET, Guntur, Andhra Pradesh, INDIA*
[3]*Department of CSE, PVPSIT, Vijayawada, Andhra Pradesh, INDIA*

Abstract:- Distributed Denial of Service (DDoS) Attacks became a massive threat to the Internet. Traditional Architecture of internet is vulnerable to the attacks like DDoS. Attacker primarily acquire his army of Zombies, then that army will be instructed by the Attacker that when to start an attack and on whom the attack should be done. In this paper, different techniques which are used to perform DDoS Attacks, Tools that were used to perform Attacks and Countermeasures in order to detect the attackers and eliminate the Bandwidth Distributed Denial of Service attacks (B-DDoS) are reviewed. DDoS Attacks were done by using various Flooding techniques which are used in DDoS attack.

The main purpose of this paper is to design an architecture which can reduce the Bandwidth Distributed Denial of service Attack and make the victim site or server available for the normal users by eliminating the zombie machines. Our Primary focus of this paper is to dispute how normal machines are turning into zombies (Bots), how attack is been initiated, DDoS attack procedure and how an organization can save their server from being a DDoS victim. In order to present this we implemented a simulated environment with Cisco switches, Routers, Firewall, some virtual machines and some Attack tools to display a real DDoS attack. By using Time scheduling, Resource Limiting, System log, Access Control List and some Modular policy Framework we stopped the attack and identified the Attacker (Bot) machines.

Keywords:- Simulation, Network Security, Botnet, DoS, DDoS, BW-DDoS, Firewall.

I. INTRODUCTION

Denial of Service (DoS) Attack means from one machine sending continuous packets of unwanted information to a server or a website. When multiple compromised machines (Zombies / Bots) try to perform DoS attack individually is called as DDoS Attack. In recent years the Bandwidth Distributed Denial of Service Attack's volume has been recorded as 300 Gbps [1]. When compared with the Q4 of 2014 and Q1 of 2015 found 35 percent increase in DDoS activity against customers, more than double number of attackers was recorded in 2015. According to the year 2014 Q4 DDoS Bandwidth has reached to 400 Gbps[2]. In 2015 Q1 DDoS attack reports the top 10 source countries which are actively participating in DDoS Attack are shown in Figure - 1.

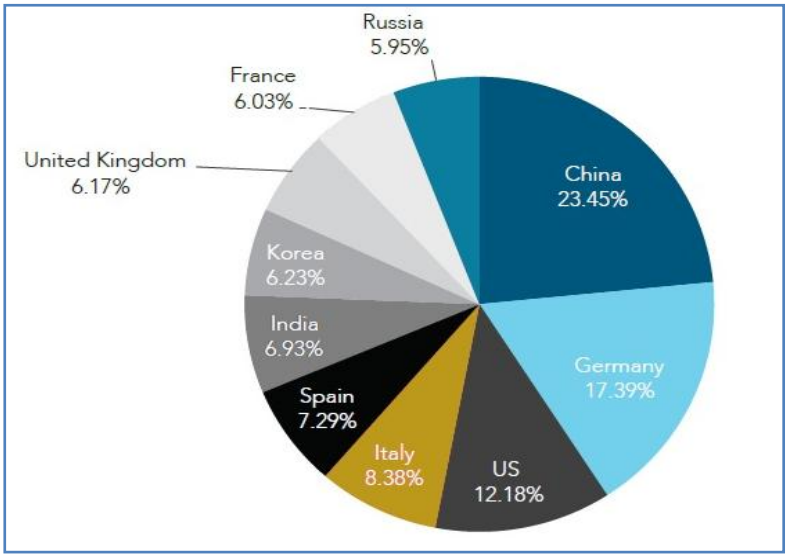

Fig. 1. Top 10 countries for DDoS attacks in 2015 Q1

From to the Figure - 1 China has become the 1st country, who is performing the largest DDoS Attack. Bandwidth was droped from 6.41 to 5.95 in 2015 Q1 report, number of attackers were decreased from Q4 2014 to Q1 2015 [3].

The main person behind the DDoS attack is Botmaster (Hacker)[1]. Primarly botmaster accquire bots (Zombies) by trapping them, Botmaster writes a malicious code into a file and embded that for not detecting it by the normal user and that will be uploaded to any website where normal user generally download information. When a normal user download that and opens it then the machine which is been used by the normal user will become a Bot. When a Botmaster wants to attack a perticular server he follows two methods [4],[5].

(i) Centralised : In centralised approach the Botmaster approaches a Command and Control (C&C) Server inorder to communicate with his bots for hiding his identity.

(ii) Decentralised : In this approach the approach Botmaster uses Peer-peer, which means making one bot as a server and makes the communication with all other bots with that master bot and making the other bots store information so that botmaster can change his server at any time this will be more effective and hard to identify the Botmaster.

By using any one of the technique from above the attack will initeate the attack with showing his identity. In this DDoS Attack the resources of the victim will be exhausted by sending unlimited packets of information with the maximum avaliable bandwidth of the bot machine. Here victim machine will recieve a hugh amount of traffic generated by the bot machines and it also receive normal traffic at the same time. It will be difficult to identify which is attacker traffic and which is normal, as the result the victim machine's resources will be exhausted and will not able to respond to the normal traffic. There are lot of companies which were effected by the DDoS attacks [1] which were lost their connection with outside world and some have lost their server which was crashed in that attack. Till now the record breaking DDoS Attack was noted as 400Gbps which happened in Europ on Dec-2014, impact of the attack was displayed in the Figure - 2, sorce from Digital Attack Map.

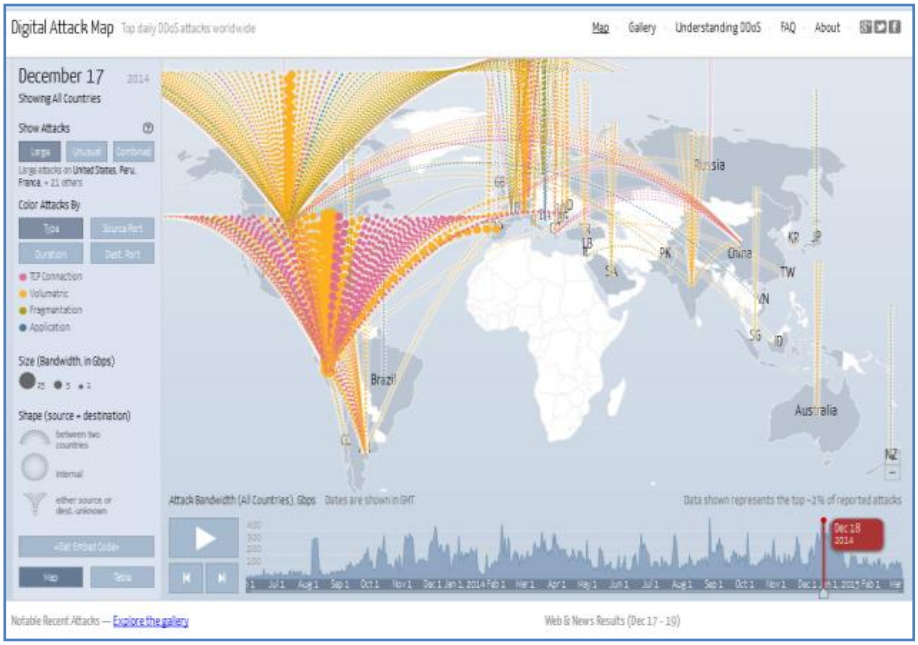

Fig. 2. Largest DDoS Attack Recorded

In digital communication every communication should pass through Hubs, switches, routers and other devices like Firewall, Inrusion Prevention System (or) Intrusion Detection System. Present the attacks were sofisticated and are using Amplifiers to manuplate the attack and increase the effect of the DDoS Attack, with the latest avaliable technologythere are lot of new tools that are helpfull in performing the attack with out identifying. In order to detect and stop the DDoS attck previously there were many techniques like IP Traceback, Probabilistic Packet Marking, Deterministic Packet Marking and many more.

II. BACKGROUND

DDoS attack will exhaust the resources of the victim by sending massive unwanted packets of information to make it busy, when ever a DDoS attack happens the bandwidth of the victim will be drined and make the services provided by the victim not avaliable for the normal users. Generally for every server their will

be capacity (or) limitation that it can provide only for certain amount of users and certain number of connection per second can only be a possiable for server and when this server was meet with a DDoS attack then if the attack is beyond the capacity of the server then it automatically fails and if the attack is been continiously been happen then their is a chance of crash of server may took place, when server gets crashed the normal users can not access the resources which are provided by the victim machine [1],[5].

2.1 Background :

In order to perform the DDoS attack the Botmaster need an army of bot's under his control by using above two senario's. When botmaster wants to attack then he will send a message M(k) to the C&C server which will pass the information to all the bots which are listed in his database. The contents of the message are listed below.

$$\mathbf{M(k) = A(t) + Dst(IP) + T} \qquad \mathbf{(1)}$$

Where:

M(k) : message from Botmaster to all Bots
A(t) : Time to start the Attack include date and time
Dst(IP) : Victim machines IP address
T : Duriation of the attack or End time

From the equaction (1), when ever the message reaches to the bot's it will wait for the Attack starting time "A(t)", at that time if that bot machine is connected to the internet then it will start the attack to the victim which was in the message. In order to perform attack Bot's will use several flooding attacks like TCP/IP flooding, UDP flooding, Syn flooding [6],[8]. Bots will automatically download the attacking tools at the background process with out knowning to the original users, when that protocol was invoked then it will start with respect to the starting time and will continue the attack with the maximum bandwidth avaliable to that machine where all bots are in communicate with other and share the information.

2.2 Why DDoS Attack

Botmaster's are motivated to perform a DDoS attack by various reasons that are benifical in financial, there are several benificets through which the attacker are intended to perform a DDoS attack [7] they are

(i) Economical Gain : Before performing the DDoS attack Botmaster will demand for hugh amount of money if botmaster does'nt get money from the intended person then he will perform the attack. Most of the DDoS attacks were done for the purpose of money.

(ii) Intellectual Challenge : young hacking enthusiasts try to prove that they are worthy and they can do better then others.

(iii) Revange : Some of the hacker wants to take their personal revange by attacking their server with a massive bot army by nullifying their server.

(iv) Ideological belief : Attackers who belong to this category are motivated by their ideological beliefs to attack their targets. This category is currently one of the major incentives for the attackers to launch DDoS attacks. For instance, political incentives have led to recent sabotages in Estonia 2007, Iran 2009 and WikiLeaks 2010.

2.3 How DDoS Attck happens

In the process of DDoS attack we can classify in to four levels Botmaster, server, Bots, victim [4], [5].

(i) Botmaster : Botmaster will send a message M(k) to the command and control server (C&C) to hide his identy.

(ii) Server : All bot's information will be placed in the server by the botmaster in his account at the server. When ever a message M(K) is recieved then it will check for the all bot's Ip-address and server will dispatch that message to all bots with respect to the Botmaster as S(M(k)).

(iii) Bots : when bots revieve the message from the server S(M(k)), then it will wait for the time to start A(t) to be arrived and when it arrives it will start the attack from the individual bots as A(D(T)) where A contain the M(k) which was sent by the Botmaster. In this process Bots may use other attacking softwares which were downloaded at the background process.

(iv) Victim : As a server it gets requests from both normal and attacker and when the traffic is beyond the range of the server then it will not be able to provide the services for any user who is trying to gain access [5].

Structure and flow of a DDoS Attack is shown below as Figure - 3.

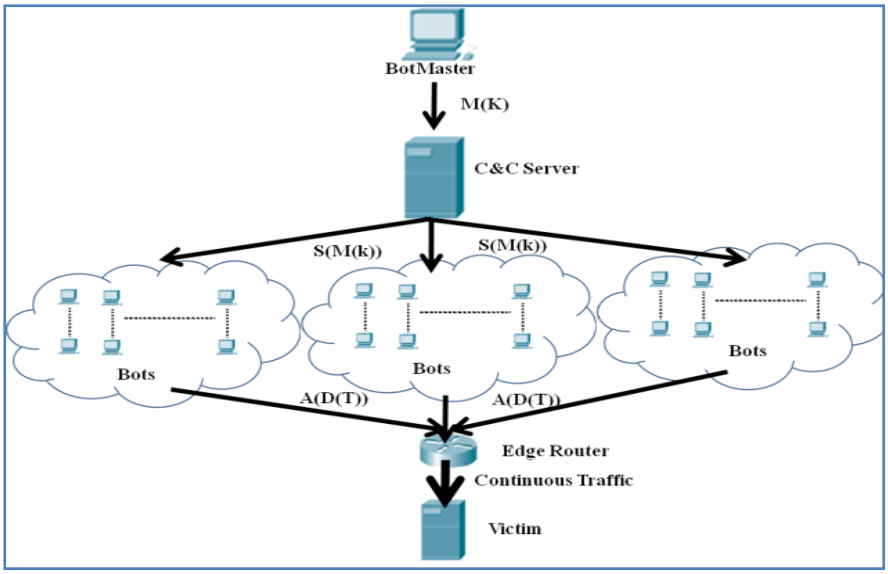

Fig. 3. Structure of DDoS Attack

Each and every communication from one network to another network should pass by a router. Here in this Figure - 3 above, Edge router is mentioned which is close enough to the server, so the default job of a router is to provide communication from one network to another network. Traffic can be restricted at router level by using Access Control Lists (ACL) but not effectively done because we can stop an IP or an Interface which is directly connected to the router can be prevented by using Router. For DDoS attacks that won't be enough to prevent the DDoS attacks. So according to the Figure - 3 the transmitted data from the router to the victim will be A(D(T)) from various networks which is from various individual machines constantly. Consider the resources of the victim as V(R) and collective bandwidth (Normal & Attacker) as B(N,A). If the V(R) < B(N,A) then their won't be any problem the server can sustain and the normal user can gain access. If the V(R) > B(N,A) then the Server cannot respond properly to the normal hence the server gets crashed [5].

In order to perform a DDoS Attack Bots need different flooding techniques which are used to send continuous packets of information to the victim machine. Basic flooding techniques are TCP Flooding, ICMP flooding UDP flooding and SYN flooding.

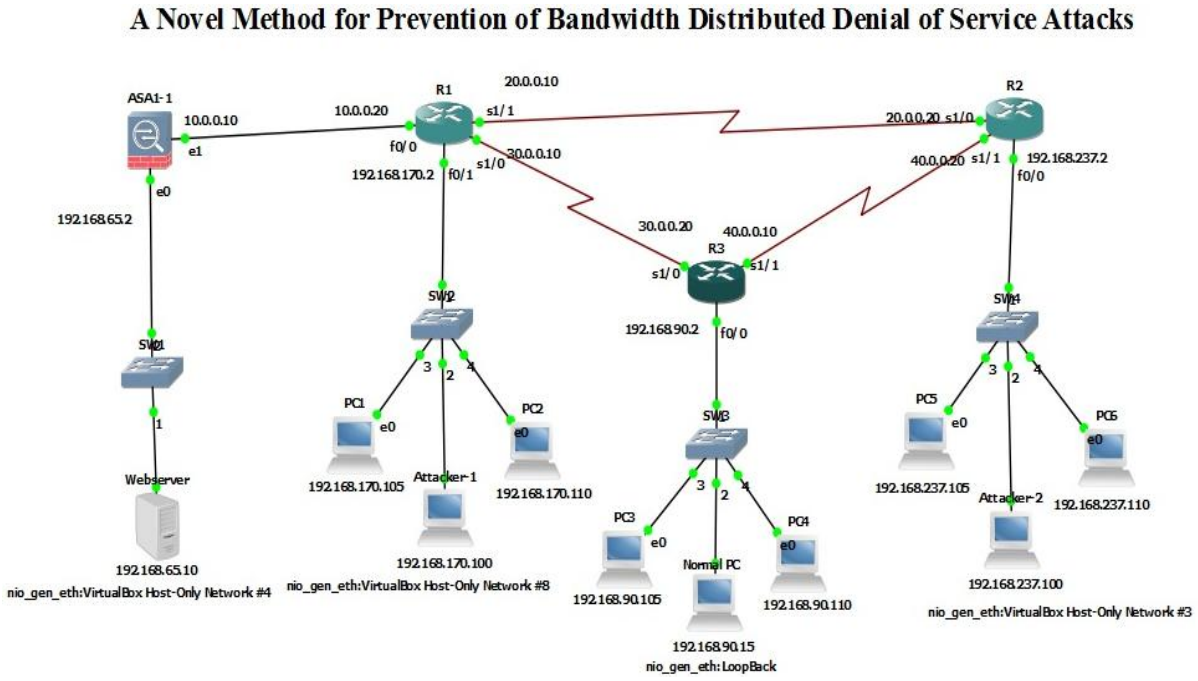

Fig. 4 Topology

III. RELATED WORK

3.1 Topology

In order to dispute a Bandwidth Distributed Denial of Service (BW-DDoS) Attacks we constructed a topology as shown in Figure - 4. Here we considered some Bots (Attacker machines) with different IP address ranges as different networks, to make the server communication with outside world we used routers with dynamic routing, so that every system in the topology can communicate with the server for acquiring services.
We created server and other attacking machines as virtual machines in Virtual Box and some are VPCs (Virtual PC's tool). For maintains we took Windows Server 2008 as the Server operating system which is a dedicated Web-Server using Internet Information Services (IIS). Attacker machines are taken as Windows 7 operating systems with which we can use all DDoS Tools in order to perform attack on the web server. All the traffic is channelled through the routers where the Shortest Path First (SPF) was mapped so even if anyone router fails the transmission will be continued from the other route. In order to amplify the attack we used different tools like Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC) [6], [9], Trinoo and some coding in python which is used to generate the traffic like HULK.py and GoldenEye.py were used.

In router we used serial connection to connect the different routers together and in order to connect the normal devices like switches and firewall Fasteathernet cables were used. For better understanding each and every network is separated with a different IP address range and the attached to a single switch when they are in same network. Firewall is placed at the very near to the server and each and every communication which is sent to server should pass only by the firewall according to our scenario. The default job of a firewall is the block all the communication from outside to inside which means server can communicate with outside networks but Outside network cannot communicate with server. It says security-level of inside interface is 100 percent but outside interface is 0 percent, so inside can communicate with outside but vice versa is not possible. In order to overcome we gave Access to outsider to communicate with inside network by using Access Control List (ACL) commands.

3.2 Attack

After analysing various techniques and available tools we used some tools to perform various flooding like Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC), Trinoo and some coding in python which is used to generate the traffic like HULK.py and GoldenEye.py were used. By using these tools in all Bot machines to perform an DDoS attack successfully. From the Figure - 4 before the attack is performed we can see the web-server is working or not by using it's IP address in a browser at any machine with "HTTP://" followed by its IP address. Once the attack is been exceeded the maximum of resources that can be provided by the server V(R), then if any normal person tries he will not be able to get the web page, in stood he will get "Service unavailable" or "408. Request timed out", so that we can understand that the attack is been happening.

Let Mk be the message sending by the Bots to the server which was really given by the Botmaster, b be the number of bots, n be the maximum number of bots then t be the time interval in which attack is been made then the capacity of attack can be calculate as shown below.

$$\int_{b=1}^{n} \int_{t=1}^{\infty} ((Mk)_t)_b \qquad \textbf{(2)}$$

3.3 Prevention

As we already seen every communication happens through routers and firewall from the above Figure - 4. Previously there are several techniques which are currently used like Probabilistic Packet Marking (PPM) [10], Deterministic Packet Marking (DPM) [11], IP-Trace-back and many more. These methods are not fully functional at the time of attack, when the attack is been happening previous methods cannot be completely eliminating the problem [1].

In order to detect and prevent the DDoS attack we placed a firewall before the server so all the communication should pass only through the firewall, so all the attack can be controlled by the firewall by using Access Control List (ACL) commands that can be on protocols and by using ACL we can restrict the other protocols which are not useful in real world communication and which make the attacker make the attack more efficiently like ICMP, which is used to check the connection is available or not, but by using ICMP the attacker can propagate the attack in a high range. Here we are running a website in a web server which is only used to publish our website with outside world, so we allowed only HTTP on port 80 and all other IP protocols were denied by using ACL commands which reduced the Hugh amount of traffic.

By using System Log information in the firewall to maintain the incoming data that is IP address of the all users (Attackers, Normal users) will be maintained for analysis purpose. By using Modular policy Framework rules which are the basic requirement of the organization that can be utilized. According to the

analysis that's been conducted every connection to the attacker uses the maximum number of sessions per second, in which for a normal user does not need too many sessions with in a second to get a website opening. So if we can limit the number of sessions per one connection then automatically the Attacker traffic will be eliminated by the Firewall. Following is the Algorithm which disputes the procedure of eliminating the DDoS Attack [12].

Algorithm:

Input:- Source incoming traffic (Attack & Normal traffic)

1. Maintain the log information at firewall.
2. Disable all traffic except HTTP Port 80 on the firewall by using ACL Commands. (If organization asks for more than HTTP, can be enabled using another ACL command)
3. Limit the number of sessions per connection (z) with respect to the time (t) in seconds by using Modular Policy Framework. The following equation can reduce the entire traffic.

$$F = \int_{x=1}^{y} \text{Host}(x) + \int_{\substack{z=1 \\ t=1}}^{n} (\text{Host}(x)_z)_t \qquad \textbf{(3)}$$

4. Detecting the attack (bots) by using the system log information, by comparing with respect to the time if the number of requests from one IP address is more than the limit (n) what we set in the firewall then it will be considered as the Attacker.

IV. PERFORMANCE ANALYSIS

Some of the experimental results from the above topology were shown below. Here the attack is been observed in the graphical representation of the firewall at the victim server by using Adaptive Security Device Manager (ASDM), which is a product of CISCO for observing the performance of the firewall in graphical mode.

As all the traffic is flowing from the Firewall we can note every communication which is passing through. The graphs recorded when the attack is happening to the server and all the traffic monitoring graphs were noted below.

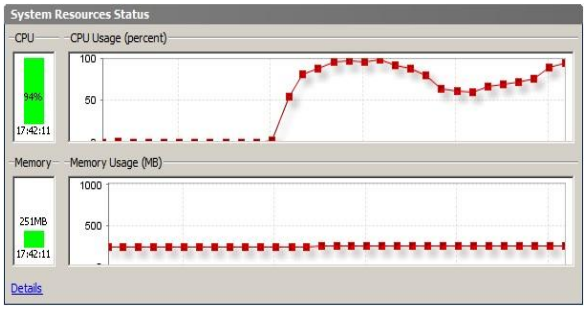

Fig. 5(a) CPU utilization when the attack is happening

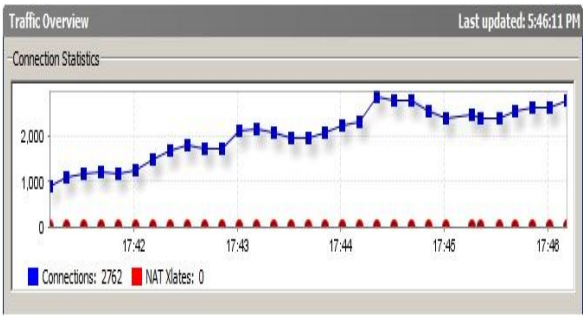

Fig. 5(b) Number of connections Established

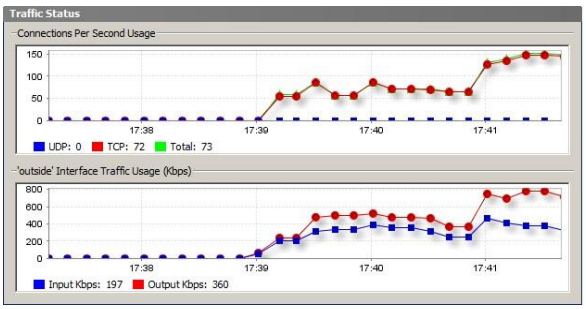

Fig. 5(c) Traffic flow from server through Firewall

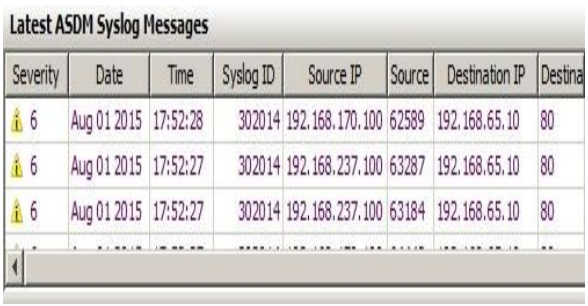

Fig. 5(d) Sys Log information when attack happening

After implementing the prevention methods at the firewall the resulted graphs are noted as follows which includes the attacker (bots) IP address and type of packets they were sending with respect to time will be recorded at the System Log information which is displayed below.

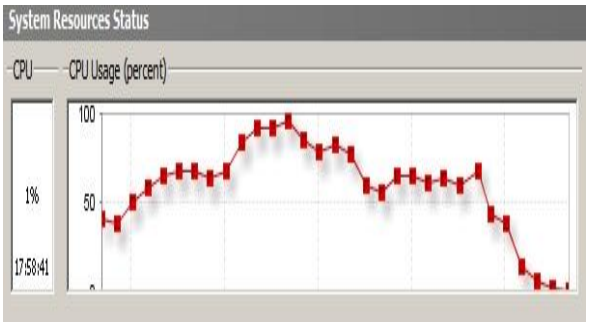

Fig. 6(a) CPU utilization after prevention

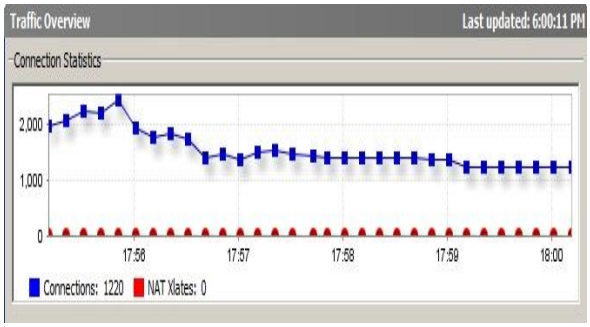

Fig. 6(b) Number of connections reduced

Fig. 6(c) Traffic flow after Prevention

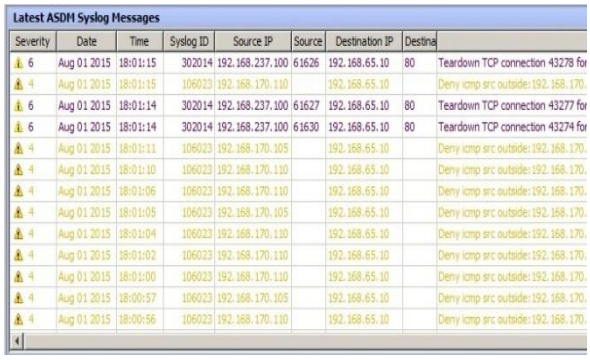

Fig. 6(d) Attackers noted in System Log

According to the comparison made between Figure - 5 and Figure - 6 we can see the constant change in the graphical representation. Here when the attack is happening then the server is not available to the normal user and when the attack is been prevented by using MPF in the firewall then automatically the utilization of the CPU became dome and the number of connection and bandwidth which is been utilized by the server became low and now the normal person can access the website from any place outside network. The attackers (bots) were noted in the System log information as noted below.

As compared with Figure - 5(d) Figure - 6(d) displays the attacker machines which are tried to attack the server, In that image we can identify attackers information like IP addresses of the Attackers, port number used, destination IP address, Destination port number and type of attack which is being happening. In the Figure - 6(d) we can observe that all the attacking traffic have been Denied by the firewall and allowing only the normal user traffic. As we already mentioned that only HTTP port -80 is allowed and remaining were denied by using ACL so except that HTTP protocol all the remaining protocols will be denied by the firewall and will not allow them to pass to the server. So the load will be reduced on server, by that it can be available for the normal users without any problem.

V. CONCLUSION AND FEATURE WORK

In this paper, we have proposed a new approach in order to detect and prevent the Bandwidth Distributed Denial of Service (BW - DDoS) Attacks. In our approach both application and network level attacks can be detected and prevented based on the Modular Policy Framework (MPF) along with the Access Control List (ACL) where the firewall is the key listener and will not allow without matching the conditions. Implementing this in the real world will give the same results where we may use any number of router, switches and Attackers. By placing a firewall before the server will always tries to defend the attacker traffic. There is a misconception that what may happen if the firewall goes down. We can use Failover concept (splitting one firewall into two firewalls by virtualization) in the firewall, when one firewall went down then automatically the other will start doing work in stood of the first one. So there won't be any disruption in the transmission but may be a little transmission delay.

As feature enhancement of this paper we propose, when the number of attackers increases then the bandwidth also increases and the load on the firewall also increases at some point the firewall may go down, so in order to obtain the better performance with better results we suggest using a Intrusion prevention System (IPS) or Intrusion Detection System (IDS) as a separate module in between the Firewall and the server in this topology. IPS uses Filtering by signature of the attack, so the firewall will do the verification and traffic reduction based on protocols and the IPS will take care of the Attacker based on their signature. Once the IPS module identify the attacker it will suspend the traffic from that machine based on the IP address, so this

approach will be more powerful and by doing this the traffic will be evaluated by both the firewall and the IPS in order to obtain the desired results.

ACKNOLEDGMENT

I would like to express my gratitude to my Project Guide G.Dayanandam, Professor, QISCET Ongole, Dr.T.V.Rao, Professor and Head of the Computer Science Department, PVPSIT, Vijayawada and Dr.P.Srinivasulu, Professor and Head of the Computer Science Department, QISCET Ongole. I also thank all the teaching staff who gave their valuable reviews and suggestions, which help me in preparing this paper.

REFERENCES

[1]. Moti geva, Amir Herzberg, and Yehoshua Gev, "Bandwidth Distribute Denial of Service Attacks and Defences," IEEE Transaction on Security & Privacy, Vol. 12, Issue. 1, Issue Date. Jan. - Feb. 2014.

[2]. Candid Wueest, "the Continued Rise of DDoS Attacks," Security Response by Symantec version 1.0 – Oct 21, 2014.]

[3]. "State of the Internet / Security" Q_1 2015 Report, Vol. 2, No. 1, May - 2015.

[4]. P.S. lokhonde, B. B. Meshram, "Botnet understanding Behaviour, Lifecycle Events & Actions," International Journal of Advance Research in Computer Science and Software Engineering. (Research paper) 2013.

[5]. Daniel Plohmann and Elmar Gerhards Padillo, "Case Study of the Miner Botnet", Cyber Conflict (CYCON), 2012.

[6]. A. Afanesyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest Flooding Attack and Counter Measures in Named Data Networking," IFIP Networking Conference, May - 2013, PP. 1-9.

[7]. Saman Taghavi zargar, James Joshi and David Tipper, "A Survay of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Communication Surveys & Tutorials, Accepted and Published 2013.

[8]. Jaeyeon Jung, Balachander Krishnamurthy, "Flash Crowds and Denial of Service Attacks: Characterization and Implementations for CDNS and Websites," Procedings of the International World Wide Web Conference, PP. 253 – 262, IEEE, May – 2002.

[9]. Aiko Pras, Anna Sperotto, Giovane C. M. Moura, Idilio Drago, Rafael Barbada, Ramin Sadre, Ricardo Schmidt and Rick Hofstede, "Attacks by Anonymous WikiLeaks Proponents not Anonymous," CTIT Technical Report PP. 10.41, Dec. 10, 2010.

[10]. Michael T. Goodrich, "Probabilistic packet Marking for Large Scale IP Trace back," IEEE/ ACM Transactions of Networking, Vol. X, Jun - 2007.

[11]. Andrey Belenky and Nirwan Ansari, "IP Traceback with Deterministic Packet Marking," IEEE Communications Letters, Vol. 7, No. 4, Apr – 2003.

[12]. Darshan Lal Meena, Dr. R. S. Jadon, "Distributed Denial of Service Attacks and their Suggested Defense Remedial Approaches", International journal of Advance Research in Computer Science and Managment Studies, vol. 2, Issue. 4, Apr – 2014.